УДК 681.32

В. П. Семеренко
О. Д. Степанов

ПРОГРАМНА РЕАЛІЗАЦІЯ CRC НА ОСНОВІ ЛІНІЙНИХ АВТОМАТІВ

Вінницький національний технічний університет

Анотація

Розглянуто особливості використання контрольних сум CRC в системах зберігання даних. Запропоновано метод обчислення CRC за допомогою теорії лінійних автоматів. Доведена можливість швидкого обчислення контрольної суми завдяки використанню паралельної обробки даних.

Ключові слова: CRC, циклічні коди, паралельні обчислення, лінійні автомати.

Abstract

The features of the use of CRC (cyclic redundancy check) in data storage systems are considered. A method for calculating CRC using the theory of linear automata is proposed. The possibility of accelerated checksum calculation due to the use of parallel data processing is proved.

Keywords: CRC, cyclic codes, parallel calculation, linear automaton

Забезпечення високої достовірності та цілісності інформації є актуальною задачею в різних галузях науки і техніки. Ця задача може бути розв'язана за допомогою завадостійкого кодування. Серед завадостійких кодів найбільш поширеними є циклічні коди, а серед циклічних кодів – коди CRC (*Cyclic Redundancy Code* – циклічний надлишковий код), який використовується, наприклад, в комп'ютерних мережах на основі протоколів Ethernet [1]. Цей код дозволяє виправляти поодинокі помилки та виявляти велику кількість інших типів помилок.

Часто достатньою вимогою є лише підтвердження факту безпомилкового передавання або збереження даних. Саме такі вимоги закладені в контрольній сумі CRC (*Cyclic Redundancy Check* – циклічний надлишковий контроль), яка використовується, наприклад, в дискових масивах RAID [2].

В подальшому будемо використовувати CRC як контрольну суму [3].

Основною практичною проблемою CRC є проблема її програмно-апаратної реалізації. Апаратна реалізація на основі лінійних регістрів зсуву функціонує з максимальною швидкістю, однак ці регістри важко (а часто і неможливо) додати до існуючих схем мікроконтролерів і мікропроцесорів.

Тому найчастіше CRC реалізують програмно. Найбільш відомими програмними методами обчислення CRC є табличні та автоматні.

Суть табличних реалізацій CRC полягає у використанні наперед підготовлених і зберігаємих проміжних результатів контрольних сум. Основний недолік табличних реалізацій – швидке зростання розмірів самих таблиць. Наприклад, для 16-розрядних CRC-16 необхідна таблиця обсягом 1 Мбайт, а для 32-розрядних CRC-32 вже необхідна таблиця обсягом 128 Гбайт [4].

Отримати ефективну програмну реалізацію CRC можна основі теорії лінійних автоматів, точніше, теорії лінійних послідовнісних схем (ЛПС) [5].

Ця математична модель над двійковим полем Галуа базується на функції переходів

$$S(t+1) = A \times S(t) + B \times U(t), \qquad (1)$$

де t – дискретний час,

A, B – характеристичні матриці ЛПС, $S(t)$ – слово стану ЛПС, $U(t)$ – вхідне слово ЛПС.

На кожному такті роботи автомата обчислюється його черговий стан $S(t)$, Останній стан $S(n)$ автомата є n-розрядним CRC. Такий метод обчислення CRC можна назвати послідовним автоматним, він може бути використаний в системах передачі даних. В цих системах швидкість формування контрольної суми відбувається синхронно з надходженням вхідних даних, тобто побітово.

Для досягнення максимальної продуктивності роботи у системах зберігання даних пропонується паралельний автоматний метод обчислення CRC. Його відмінність від попереднього полягає у використанні функції переходів

$$S(t+m) = A^m \times S(t) + B \times U(t) \quad (2)$$

Функція (2) використовує складніші характеристичні матриці A та B і обчислює проміжні значення CRC не побітово, а групами по m біт. В результаті швидкість обчислень зростає в n/m разів, в витрати пам'яті зменшуються в n/m разів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Столлингс В. Компьютерные системы передачи данных. Изд. 6-е; пер. с англ. – М., Издательский дом «Вильямс», 2002. – 928 с.
2. *Patterson, D. A.* A Case for Redundant Arrays of Inexpensive Disks (RAID) : // SIGMOD '88 : Proceedings of the 1988 ACM SIGMOD international conference on Management of data : D. A. Patterson, G. Gibson, R. H. Katz. — 1988. — June. — P. 109–116.
3. Semerenko, V. P "Theory and Practice of CRC Codes : New Results Based on Automaton Models," *in Eastern-European Journal of Enterprise Technologies*, vol. 4, issue 9 (76), 2015, pp. 38–48. doi: 10.15587/1729-4061.2015.47860
4. Мыцко Е.А., Мальчуков А.Н. Особенности аппаратной реализации алгоритмов вычисления контрольной суммы CS32 // Вестник науки Сибири, 2012. – №. 5 (6). – С. 87-92.
5. Семеренко В. П. Теорія циклічних кодів на основі автоматних моделей : монографія. Вінниця : ВНТУ, 2015. – 444 с.

Василь Петрович Семеренко – канд. техн. наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: vasilsemerenko@gmail.com

Олексій Дмитрович Степанов – студент групи 2КІ-18б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця
e-mail: Stepanovod2001@gmail.com

Vasyl P. Semerenko – PhD, Associate Professor, Department of computer technique, Vinnytsia National Technical University, Vinnytsia, e-mail: vasilsemerenko@gmail.com

Oleksii D. Stepanov – student, Department of computer technique, Vinnytsia National Technical University, Vinnytsia. e-mail: Stepanovod2001@gmail.com